The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
03/12/2013

SUBJECT:
Vulnerabilities in Microsoft Visio Viewer 2010 Could Allow Remote Code Execution (MS13-023)

OVERVIEW:
A vulnerability in Microsoft Visio Viewer 2010 has been identified that could allow for remote code execution. Microsoft Visio Viewer is a program commonly used to view flowcharts, network diagrams and other visual media that can be used in Office-based products. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:
- Microsoft Visio Viewer 2010

RISK:

Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: Medium

DESCRIPTION:
A vulnerability has been identified in Microsoft Visio Viewer 2010 that could result in remote code execution. This vulnerability exists due to the way Microsoft Visio Viewer 2010 handles memory when rendering specially crafted Visio files.

Exploitation may occur via an e-mail-based attack scenario or a web-based attack scenario. In an e-mail-based scenario, a user would have to open a specially crafted Visio file as an e-mail

attachment. In a web-based scenario, a user would have to visit a website and open a specially crafted Visio file.

Successful exploitation could allow an attacker to gain the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by attachments and hypertext links contained in emails especially from un-trusted sources.

References:

Microsoft:
http://technet.microsoft.com/en-us/security/bulletin/ms13-023

Security Focus:
http://www.securityfocus.com/bid/58369

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-0079